

Elaine A. Ryan (AZ Bar #012870)
Colleen M. Auer (AZ Bar#014637)
AUER RYAN, P.C.
20987 N. John Wayne Parkway, #B104-374
Maricopa, AZ 85139
520-705-7332
eryan@auer-ryan.com
cauer@auer-ryan.com

**IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ARIZONA**

Flor Medina and Doreen Barbieri on
behalf of the Estate of Mario Barbieri, on
behalf of themselves and others similarly
situated,

Plaintiffs,

v.

PracticeMax, Inc., a Delaware
corporation,

Defendant.

Case No.

CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Plaintiffs Flor Medina (“Ms. Medina”) and Doreen Barbieri (“Ms. Barbieri”), on behalf of her late father Mario Barbieri’s estate, (collectively “Plaintiffs”) bring this Class Action Complaint on behalf of themselves, and all others similarly situated against Defendant PracticeMax Inc. (“PracticeMax” or “Defendant”), and its present, former, or future direct and indirect parent companies, subsidiaries, affiliates, agents, and/or other related entities, and allege as follows:

NATURE OF THE ACTION

1. On May 1, 2021, Defendant PracticeMax, a medical practice management firm providing billing, consulting, and registration services to hospitals and healthcare

1 providers, identified a cyberattack of its systems. Cybercriminals had unrestricted access
 2 to PracticeMax's files and systems from April 17, 2021 to May 5, 2021 (the "Data
 3 Breach").

4 2. As a result, PracticeMax lost control of highly-sensitive files belonging to
 5 over 150,000 patients that contained personal health information ("PHI")¹, including
 6 names, addresses, Social Security numbers, dates of birth, treatment and/or diagnosis
 7 information, health insurance information, and private financial information for individuals
 8 associated with PracticeMax's customers.

9 3. Not only did PracticeMax fail to properly protect its customers' patients'
 10 PHI, PracticeMax failed to timely notify victims of the Data Breach.

11 4. On information and belief, PracticeMax began notifying victims about the
 12 Data Breach on or around October 19, 2021—over five months after discovering the
 13 breach. PracticeMax has provided additional notices of the breach since then, with the latest
 14 notice provided as recently as June 10, 2022. PracticeMax has failed to explain why it has
 15 taken over a year to notify all breach victims.

18 ¹ Under the Health Insurance Portability and Accountability Act, 42 U.S.C. § 1320d
 19 *et seq.*, and its implementing regulations ("HIPAA"), "protected health information" is
 20 defined as individually identifiable information relating to the past, present, or future health
 21 status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-
 22 covered entity in relation to the provision of healthcare, payment for healthcare services,
 23 or use in healthcare operations. 45 C.F.R. § 160.103 *Protected health information*. A
 24 "covered entity" is further defined as, *inter alia*, a health care provider who transmits any
 25 health information in electronic form in connection with a transaction covered by HIPAA.
 26 *Id. Covered entity*. Health information such as diagnoses, treatment information, medical
 27 test results, and prescription information are considered protected health information under
 28 HIPAA, as are national identification numbers and demographic information such as birth
 dates, gender, ethnicity, and contact and emergency contact information. *Summary of the
 HIPAA Privacy Rule*, DEP'T FOR HEALTH & HUM. SERVS., <https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html> (last accessed June 21, 2022).
 PracticeMax is clearly a "covered entity" and some of the data compromised in the Data
 Breach that this action arises out of is "protected health information", subject to HIPAA.

1 5. When PracticeMax finally announced the Data Breach, it deliberately
2 underplayed the Breach's severity and obfuscated the nature of the Breach. PracticeMax's
3 Breach Notice sent to patients fails to explain how many people were impacted, how the
4 breach happened, or why it took over five months to send a bare-bones notice to impacted
5 patients.

6 6. On information and belief, cybercriminals were able to breach PracticeMax's
7 systems because PracticeMax did not maintain reasonable security safeguards or protocols
8 to protect patients' PHI, leaving it an unguarded target for theft and misuse. In fact,
9 PracticeMax confirms as much in its Breach Notice: "As part of PracticeMax's ongoing
10 commitment to the privacy of information in our care, we reviewed our existing policies
11 and procedures and implemented additional safeguards to further our already stringent
12 security policies and procedures and to secure the information in our systems."²

13 7. PracticeMax's failure to timely detect and notify breach victims violates
14 Arizona law and has made its patients vulnerable to identity theft without any warnings to
15 monitor their financial accounts or credit reports to prevent unauthorized use of their PHI.

16 8. On information and belief, PracticeMax has failed to offer complimentary
17 credit monitoring and identity protection services to victims of the Data Breach and has
18 instead provided rudimentary instructions for victims to monitor their own credit reports.
19 Exh. A.

20 9. PracticeMax knew or should have known that each victim of the Data Breach
21 deserved prompt and efficient notice of the Data Breach and meaningful assistance in
22 mitigating the effects of PHI misuse.

23 10. PracticeMax's misconduct has injured the Plaintiffs and members of the
24 proposed Class, including: (i) the lost or diminished value of their PHI; (ii) costs associated

25
26 ² A true and accurate copy of the Breach Notice is attached to this complaint as
27 **Exhibit A**. See <https://apps.web.maine.gov/online/aeviewer/ME/40/f3f3fcf1-7bee-45cc-a959-5fb886bf6ee1.shtml> (last accessed July 25, 2022).

1 with the prevention, detection, and recovery from identity theft, tax fraud, and other
2 unauthorized use of their data; (iii) lost opportunity costs to mitigate the Data Breach's
3 consequences, including lost time; and (iv) emotional distress associated with the loss of
4 control over their highly sensitive PHI.

5 11. Plaintiffs and members of the proposed Class are victims of Defendant's
6 negligence and inadequate cyber security measures. Defendant failed to properly use up-
7 to-date security practices to prevent the Data Breach.

8 12. Plaintiffs and members of the proposed Class therefore bring this lawsuit
9 seeking damages and relief for Defendant's actions.

10 **PARTIES**

11 13. Plaintiff Flor Medina is a natural person and adult citizen of Arizona, residing
12 in Tolleson, Arizona. In early June 2022, Ms. Medina received notice of the data breach
13 from Defendant PracticeMax stating that her PHI was compromised by the Data Breach.

14 14. Plaintiff Doreen Barbieri is a natural person and adult citizen of Illinois,
15 residing in Chicago, Illinois. Ms. Barbieri is the executor of Mr. Mario Barbieri's estate.
16 Ms. Barbieri received the Defendant's Notice of Breach letter directed to Mario Barbieri
17 in June 2022 stating that her late father's PHI was compromised by the Data Breach.

18 15. Defendant PracticeMax is a Delaware corporation with its principal place of
19 business at 1440 E. Missouri Ave, Suite C-200, Phoenix, Arizona 85364. PracticeMax has
20 additional facilities located throughout the country, including but not limited to Louisiana,
21 New York, and Illinois.

22 **JURISDICTION AND VENUE**

23 16. This Court has subject matter jurisdiction over this action under 28 U.S.C. §
24 1332(d) because this is a class action in which the amount in controversy exceeds \$5
25 million, exclusive of costs and interest, there are more than 100 members in the proposed
26

1 class, and at least one class member is a citizen of a different state than PracticeMax,
2 establishing minimal diversity.

3 17. This Court has personal jurisdiction over PracticeMax because it is
4 headquartered in Phoenix, Arizona.

5 18. Venue is proper in this Court under 28 U.S.C. §§ 1391 because a substantial
6 part of the alleged wrongful conduct and events giving rise to the claims occurred in this
7 District and because PracticeMax conducts business in this District.

8 **FACTUAL ALLEGATIONS**

9 **A. PracticeMax's Failure to Safeguard Patients' PHI**

10 19. Plaintiffs and members of the proposed Class are PracticeMax's customers'
11 current and former patients.

12 20. As a prerequisite of receiving treatment, PracticeMax's customers require
13 their patients to provide their PHI. PracticeMax admits to collecting patients' demographic
14 and sensitive health information. Exh. A.

15 21. On information and belief, PracticeMax maintains records of its customers'
16 patients' information such as patients' full names, Social Security Numbers, financial
17 account information and/or credit-card information, dates of birth, prescription
18 information, diagnosis information, treatment information, treatment providers, health
19 insurance information, medical information, and Medicare/Medicaid ID numbers, in the
20 ordinary course of business. These records are stored on PracticeMax's computer systems.

21 22. When PracticeMax collects this sensitive information, it promises to use
22 reasonable measures to safeguard the PHI from theft and misuse.

23 23. Despite its alleged commitments to securing sensitive patient data,
24 PracticeMax does not follow industry standard practices in securing patients' PHI.

25 24. In April 2021, hackers bypassed PracticeMax's security safeguards and
26 infiltrated its systems, giving them unfettered access to current and former patients' PHI.
27
28

1 25. The unauthorized individuals had access to patients' PHI from April 17,
2 2021, to May 5, 2021, and removed files from PracticeMax's systems. Exh. A.

3 26. In response to the Data Breach, PracticeMax contends that it "implemented
4 additional safeguards to further [its] . . . security policies and procedures and to secure the
5 information in [its] systems." Exh. A. These additional security measures should have been
6 in place *before* the Data Breach.

7 27. PracticeMax's Breach Notice letter, as well as its website notice, both omit
8 the size and scope of the breach. PracticeMax has demonstrated a pattern of providing
9 inadequate notices and disclosures about the Data Breach.

10 28. On information and belief, the Data Breach has impacted at least 150,000
11 former and current patients.

12 29. On information and belief, PracticeMax does not adequately train its
13 employees on cybersecurity policies, enforce those policies, or maintain reasonable
14 security practices and systems.

15 30. PracticeMax's negligent conduct caused the Data Breach. PracticeMax
16 violated its obligation to implement best practices and comply with industry standards
17 concerning computer system security. PracticeMax failed to comply with security
18 standards and allowed patients' PHI to be accessed and stolen by failing to implement
19 security measures that could have prevented, mitigated, or timely detected the Data Breach.

20 31. On information and belief, PracticeMax notified victims of the Data Breach
21 that their PHI was accessed in the breach via notice letters resembling the Breach Notice
22 attached hereto as Exhibit A.

23 32. PracticeMax recommends for Data Breach victims to "remain vigilant by
24 reviewing documents for suspicious activity, including health insurance statements,
25 explanation of benefits of letters, medical records, account statements and credit reports."
26 Exh. A.

1 33. What PracticeMax did not do is provide any credit monitoring or other
2 support services to victims of the Data Breach. Rather, PracticeMax provides general
3 instructions to victims to mitigate the consequences of PracticeMax's negligence in
4 allowing the Data Breach to occur, and its failures to detect the same for approximately
5 eighteen days.

6 **B. Plaintiff Medina's Experience**

7 34. Plaintiff Medina is a former patient of one of PracticeMax's customers.

8 35. Ms. Medina is unfamiliar with PracticeMax and never authorized
9 PracticeMax's collection of her PHI.

10 36. In early June 2022, Ms. Medina received a Breach Notice letter in the mail.

11 37. As a result of the Data Breach notice, Ms. Medina spent time dealing with
12 the consequences of the Data Breach, which includes time spent verifying the legitimacy
13 of the Notice of Data Breach, self-monitoring her accounts and credit reports to ensure no
14 fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

15 38. Ms. Medina suffered actual injury in the form of damages to and diminution
16 in the value of her PHI, which was compromised in and as a result of the Data Breach.

17 39. Ms. Medina will have to spend considerable time and effort over the coming
18 years monitoring her accounts to protect herself from identity theft. Ms. Medina's personal
19 financial security has been jeopardized and there is uncertainty over what medical
20 information was revealed in the Data Breach.

21 40. Ms. Medina's sensitive PHI remains in PracticeMax's possession without
22 adequate protection against known threats, exposing Plaintiff to the prospect of additional
23 harm in the event PracticeMax suffers another data breach. Thus, Ms. Medina has a
24 continuing interest in ensuring that her PHI is protected and safeguarded from future
25 breaches.

C. Plaintiff Doreen Barbieri and Mario Barbieri's Experience

41. Plaintiff Doreen Barbieri is the executor of her late father's estate.

42. The decedent, Mario Barbieri, was a patient of one of the Defendant's customers between 2008 and 2020. Mr. Mario Barbieri passed away in 2020.

43. Mr. Mario Barbieri lived with Ms. Barbieri for over twenty years before his passing. Ms. Barbieri is familiar with her late father's medical history and his estate.

44. In early June 2022, Ms. Barbieri received a Breach Notice letter in the mail indicating her late father's PHI was compromised in the Data Breach.

45. As a result of the Data Breach notice, Ms. Barbieri spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Breach, self-monitoring her late father's estate accounts to ensure no fraudulent activity has occurred. This time has been lost forever and cannot be recaptured.

46. Ms. Barbieri has recently become bombarded by spam phone calls relating to her late father, who lived at her residence and used the same landline telephone number as Ms. Barbieri.

D. Plaintiffs and the Proposed Class Face Significant Risk of Continued Identity Theft

47. Plaintiffs and members of the proposed Class have suffered injury from the misuse of their PHI that can be directly traced to Defendant.

48. The ramifications of Defendant's failure to keep Plaintiffs' and the Class's PHI secure are severe. Identity theft occurs when someone uses another's personal and financial information such as that person's name, account number, Social Security number, driver's license number, date of birth, and/or other information, without permission, to commit fraud or other crimes.

49. According to experts, one out of four data breach notification recipients become a victim of identity fraud.³

50. As a result of Defendant's failures to prevent—and to timely detect—the Data Breach, Plaintiffs and the proposed Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PHI is used;
- b. The diminution in value of their PHI;
- c. The compromise and continuing publication of their PHI;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PHI; and
- h. The continued risk to their PHI, which remains in the possession of PracticeMax and is subject to further breaches so long as PracticeMax fails to undertake the appropriate measures to protect the PHI in their possession.

³ *Study Shows One in Four Who Receive Data Breach Letter Become Fraud Victims*, ThreatPost.com (Feb. 21, 2013), <https://threatpost.com/study-shows-one-four-who-receive-data-breach-letter-become-fraud-victims-022013/77549/> (last visited July 25, 2022).

1 51. Stolen PHI is one of the most valuable commodities on the criminal
2 information black market. According to Experian, a credit-monitoring service, stolen PHI
3 can be worth up to \$1,000.00 depending on the type of information obtained.⁴

4 52. The value of Plaintiffs' and the proposed Class's PHI on the black market is
5 considerable. Stolen PHI trades on the black market for years, and criminals frequently
6 post stolen private information openly and directly on various "dark web" internet
7 websites, making the information publicly available, for a substantial fee of course.

8 53. It can take victims years to spot or identify PHI theft, giving criminals plenty
9 of time to milk that information for cash.

10 54. One such example of criminals using PHI for profit is the development of
11 "Fullz" packages.⁵

12 55. Cyber-criminals can cross-reference two sources of PHI to marry
13 unregulated data available elsewhere to criminally stolen data with an astonishingly
14 complete scope and degree of accuracy in order to assemble complete dossiers on
15 individuals. These dossiers are known as "Fullz" packages.

17 ⁴ See Here's How Much Your Personal Information Is Selling for on the Dark Web,
18 Experian, <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last visited July 25, 2022).

19 ⁵ "Fullz" is fraudster speak for data that includes the information of the victim,
20 including, but not limited to, the name, address, credit card information, social security
21 number, date of birth, and more. As a rule of thumb, the more information you have on a
22 victim, the more money can be made off those credentials. Fullz are usually pricier than
23 standard credit card credentials, commanding up to \$100 per record or more on the dark
24 web. Fullz can be cashed out (turning credentials into money) in various ways, including
25 performing bank transactions over the phone with the required authentication details in-
26 hand. Even "dead Fullz", which are Fullz credentials associated with credit cards that are
27 no longer valid, can still be used for numerous purposes, including tax refund scams,
28 ordering credit cards on behalf of the victim, or opening a "mule account" (an account that
will accept a fraudulent money transfer from a compromised account) without the victim's
knowledge. See, e.g., Brian Krebs, *Medical Records For Sale in Underground Stolen From
Texas Life Insurance Firm*, KREBS ON SECURITY, (Sep. 18, 2014), available at
<https://krebsonsecurity.com/tag/fullz/>, (last visited July 25, 2022).

1 56. The development of “Fullz” packages means that stolen PHI from the Data
2 Breach can easily be used to link and identify it to Plaintiff’s and the proposed Class’s
3 phone numbers, email addresses, and other unregulated sources and identifiers. In other
4 words, even if certain information such as emails, phone numbers, or credit card numbers
5 may not be included in the PHI stolen by the cyber-criminals in the Data Breach, criminals
6 can easily create a Fullz package and sell it at a higher price to unscrupulous operators and
7 criminals (such as illegal and scam telemarketers) over and over. That is exactly what is
8 happening to Plaintiffs and members of the proposed Class, and it is reasonable for any
9 trier of fact, including this Court or a jury, to find that Plaintiff’s and other members of the
10 proposed Class’s stolen PHI is being misused, and that such misuse is fairly traceable to
11 the Data Breach.

12 57. According to the FBI’s Internet Crime Complaint Center (IC3) 2019 Internet
13 Crime Report, Internet-enabled crimes reached their highest number of complaints and
14 dollar losses that year, resulting in more than \$3.5 billion in losses to individuals and
15 business victims.

16 58. Further, according to the same report, “rapid reporting can help law
17 enforcement stop fraudulent transactions before a victim loses the money for good.”
18 Defendant did not rapidly report to Plaintiffs and the Class that their PHI had been stolen.

19 59. Victims of identity theft also often suffer embarrassment, blackmail, or
20 harassment in person or online, and/or experience financial losses resulting from
21 fraudulently opened accounts or misuse of existing accounts.

22 60. In addition to out-of-pocket expenses that can exceed thousands of dollars
23 and the emotional toll identity theft can take, some victims have to spend a considerable
24 time repairing the damage caused by the theft of their PHI. Victims of new account identity
25 theft will likely have to spend time correcting fraudulent information in their credit reports
26 and continuously monitor their reports for future inaccuracies, close existing bank/credit
27 accounts, open new ones, and dispute charges with creditors.
28

61. Further complicating the issues faced by victims of identity theft, data thieves may wait years before attempting to use the stolen PHI. To protect themselves, Plaintiffs and the Class will need to remain vigilant against unauthorized data use for years or even decades to come.

62. The Federal Trade Commission (“FTC”) has also recognized that consumer data is a new and valuable form of currency. In a FTC roundtable presentation, former Commissioner Pamela Jones Harbour stated that “most consumers cannot begin to comprehend the types and amount of information collected by businesses, or why their information may be commercially valuable. Data is currency.”⁶

63. The FTC has also issued numerous guidelines for businesses that highlight the importance of reasonable data security practices. The FTC has noted the need to factor data security into all business decision-making.⁷ According to the FTC, data security requires: (1) encrypting information stored on computer networks; (2) retaining payment card information only as long as necessary; (3) properly disposing of personal information that is no longer needed; (4) limiting administrative access to business systems; (5) using industry-tested and accepted methods for securing data; (6) monitoring activity on networks to uncover unapproved activity; (7) verifying that privacy and security features function properly; (8) testing for common vulnerabilities; and (9) updating and patching third-party software.⁸

64. According to the FTC, unauthorized PHI disclosures are extremely damaging to consumers’ finances, credit history and reputation, and can take time, money and

⁶ Statement of FTC Commissioner Pamela Jones Harbour—Remarks Before FTC Exploring Privacy Roundtable, (Dec. 7, 2009), <http://www.ftc.gov/speeches/harbour/091207privacyroundtable.pdf> (last visited June 21, 2022).

⁷ *Start With Security, A Guide for Business*, FTC, <https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf> (last visited July 25, 2022).

⁸ *Id.*

1 patience to resolve the fallout.⁹ The FTC treats the failure to employ reasonable and
 2 appropriate measures to protect against unauthorized access to confidential consumer data
 3 as an unfair act or practice prohibited by Section 5(a) of the FTC Act.

4 65. To that end, the FTC has issued orders against businesses that failed to
 5 employ reasonable measures to secure sensitive payment card data. *See In the matter of*
 6 *Lookout Services, Inc.*, No. C-4326, ¶ 7 (June 15, 2011) (“[Defendant] allowed users to
 7 bypass authentication procedures” and “failed to employ sufficient measures to detect and
 8 prevent unauthorized access to computer networks, such as employing an intrusion
 9 detection system and monitoring system logs.”); *In the matter of DSW, Inc.*, No. C-4157,
 10 ¶ 7 (Mar. 7, 2006) (“[Defendant] failed to employ sufficient measures to detect
 11 unauthorized access.”); *In the matter of The TJX Cos., Inc.*, No. C-4227 (Jul. 29, 2008)
 12 (“[R]espondent stored . . . personal information obtained to verify checks and process
 13 unreceipted returns in clear text on its in-store and corporate networks[,]” “did not require
 14 network administrators . . . to use different passwords to access different programs,
 15 computers, and networks[,]” and “failed to employ sufficient measures to detect and
 16 prevent unauthorized access to computer networks . . .”); *In the matter of Dave & Buster’s*
 17 *Inc.*, No. C-4291 (May 20, 2010) (“[Defendant] failed to monitor and filter outbound traffic
 18 from its networks to identify and block export of sensitive personal information without
 19 authorization” and “failed to use readily available security measures to limit access
 20 between instore networks . . .”). These orders, which all preceded the Data Breach, further
 21 clarify the measures businesses must take to meet their data security obligations.
 22 PracticeMax thus knew or should have known that its data security protocols were
 23 inadequate and were likely to result in the unauthorized access to and/or theft of PHI.

24
 25 ⁹ See Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012),
 26 [https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity](https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen)
 27 [-stolen](https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen) (last accessed July 25, 2022).

66. The healthcare industry is a prime target for data breaches.

67. Over the past several years, data breaches have become alarmingly commonplace. In 2016, the number of data breaches in the U.S. exceeded 1,000, a 40% increase from 2015.¹⁰ The next year, that number increased by nearly 45%.¹¹ The following year the healthcare sector was the second easiest “mark” among all major sectors and categorically had the most widespread exposure per data breach.¹²

68. Data breaches within the healthcare industry continued to increase rapidly. According to the 2019 Healthcare Information and Management Systems Society Cybersecurity Survey, 68% of participating vendors reported having a significant security incident within the last 12 months, with a majority of those being caused by “bad actors.”¹³

69. The healthcare sector reported the second largest number of breaches among all measured sectors in 2018, with the highest rate of exposure per breach.¹⁴ Indeed, when compromised, healthcare related data is among the most sensitive and personally consequential. A report focusing on healthcare breaches found that the “average total cost to resolve an identity theft-related incident . . . came to about \$20,000,” and that the victims were often forced to pay out-of-pocket costs for healthcare they did not receive in order to

¹⁰ *Data Breaches Increase 40 Percent in 2016, Finds New Report From Identity Theft Resource Center and CyberScout*, IDENTITY THEFT RESOURCE CENTER (“ITRC”) (Jan. 19, 2017), <https://bit.ly/30Gew91> [hereinafter “*Data Breaches Increase 40 Percent in 2016*”] (last accessed July 25, 2022).

¹¹ *Data Breaches Up Nearly 45 Percent According to Annual Review by Identity Theft Resource Center® and CyberScout®*, ITRC (Jan. 22, 2018), <https://bit.ly/3jdGcYR> [hereinafter “*Data Breaches Up Nearly 45 Percent*”] (last accessed July 25, 2022).

¹² *2018 End-of-Year Data Breach Report*, ITRC (Feb. 20, 2019), https://www.idtheftcenter.org/wp-content/uploads/2019/02/ITRC_2018-End-of-Year-Aftermath_FINAL_V2_combinedWEB.pdf. (last accessed July 25, 2022).

¹³ *2019 HIMSS Cybersecurity Survey*, HEALTHCARE INFORMATION AND MANAGEMENT SYSTEMS SOCIETY, INC. (Feb. 8, 2019), <https://bit.ly/3LJqUr6> (last accessed July 25, 2022).

¹⁴ *2018 End-of-Year Data Breach Report*.

1 restore coverage.¹⁵ Almost 50 percent of the victims lost their healthcare coverage as a
 2 result of the incident, while nearly 30 percent said their insurance premiums went up after
 3 the event. Forty percent of the customers were never able to resolve their identity theft at
 4 all. Data breaches and identity theft have a crippling effect on individuals and detrimentally
 5 impact the economy as a whole.¹⁶

6 70. The healthcare industry has “emerged as a primary target because [it sits] on
 7 a gold mine of sensitive personally identifiable information for thousands of patients at any
 8 given time. From social security and insurance policies to next of kin and credit cards, no
 9 other organization, including credit bureaus, ha[s] so much monetizable information stored
 10 in their data centers.”¹⁷

11 71. Charged with handling highly sensitive Personal Information including
 12 healthcare information, financial information, and insurance information, Defendant knew
 13 or should have known the importance of safeguarding the Personal Information that was
 14 entrusted to it. Defendant also knew or should have known of the foreseeable consequences
 15 if its data security systems were breached. This includes the significant costs that would be
 16 imposed on Defendant’s customers’ patients as a result of a breach. Defendant nevertheless
 17 failed to take adequate cybersecurity measures to prevent the Data Breach from occurring.

18 72. Defendant disclosed the PHI of Plaintiffs and members of the proposed Class
 19 for criminals to use in the conduct of criminal activity. Specifically, Defendant opened up,
 20 disclosed, and exposed the PHI of Plaintiffs and members of the proposed Class to people
 21 engaged in disruptive and unlawful business practices and tactics, including online account
 22

23 ¹⁵ Elinor Mills, *Study: Medical Identity Theft Is Costly for Victims*, CNET (Mar. 3,
 24 2010), <https://cnet.co/33uiV0v> (last accessed July 25, 2022).

25 ¹⁶ *Id.*

26 ¹⁷ Eyal Benishti, *How to Safeguard Hospital Data from Email Spoofing Attacks*,
 27 INSIDE DIGITAL HEALTH (Apr. 4, 2019), <https://bit.ly/3x6fz08> (last accessed July 25, 2022).
 28

1 hacking, unauthorized use of financial accounts, and fraudulent attempts to open
2 unauthorized financial accounts (i.e., identity fraud), all using the stolen PHI.

3 73. Defendant's use of outdated and insecure computer systems and software
4 that are easy to hack, and its failure to maintain adequate security measures and an up-to-
5 date technology security strategy, demonstrates a willful and conscious disregard for
6 privacy, and has exposed the PHI of Plaintiffs and potentially thousands of members of the
7 proposed Class to unscrupulous operators, con artists and outright criminals.

8 74. Defendant's failure to properly notify Plaintiffs and members of the proposed
9 Class of the Data Breach exacerbated Plaintiffs' and members of the proposed Class's
10 injury by depriving them of the earliest ability to take appropriate measures to protect their
11 PHI and take other necessary steps to mitigate the harm caused by the Data Breach.

12 **E. PracticeMax Failed to Adhere to HIPAA**

13 75. HIPAA circumscribes security provisions and data privacy responsibilities
14 designed to keep patients' medical information safe. HIPAA compliance provisions,
15 commonly known as the Administrative Simplification Rules, establish national standards
16 for electronic transactions and code sets to maintain the privacy and security of protected
17 health information.¹⁸

18 76. HIPAA provides specific privacy rules that require comprehensive
19 administrative, physical, and technical safeguards to ensure the confidentiality, integrity,
20 and security of PHI is properly maintained.¹⁹

21
22
23 ¹⁸ HIPAA lists 18 types of information that qualify as PHI according to guidance from
24 the Department of Health and Human Services Office for Civil Rights, and includes, *inter*
alia: names, addresses, any dates including dates of birth, Social Security numbers, and
medical record numbers.

25 ¹⁹ See 45 C.F.R. § 164.306 (Security standards and General rules); 45 C.F.R. § 164.308
26 (Administrative safeguards); 45 C.F.R. § 164.310 (Physical safeguards); 45 C.F.R. §
164.312 (Technical safeguards).

1 77. The Data Breach itself resulted from a combination of inadequacies showing
2 PracticeMax failed to comply with safeguards mandated by HIPAA. PracticeMax's
3 security failures include, but are not limited to:

- 4 a. Failing to ensure the confidentiality and integrity of electronic PHI that it
5 creates, receives, maintains and transmits in violation of 45 C.F.R. §
6 164.306(a)(1);
- 7 b. Failing to protect against any reasonably-anticipated threats or hazards to the
8 security or integrity of electronic PHI in violation of 45 C.F.R. §
9 164.306(a)(2);
- 10 c. Failing to protect against any reasonably anticipated uses or disclosures of
11 electronic PHI that are not permitted under the privacy rules regarding
12 individually identifiable health information in violation of 45 C.F.R. §
13 164.306(a)(3);
- 14 d. Failing to ensure compliance with HIPAA security standards by
15 PracticeMax's workforce in violation of 45 C.F.R. § 164.306(a)(4);
- 16 e. Failing to implement technical policies and procedures for electronic
17 information systems that maintain electronic PHI to allow access only to
18 those persons or software programs that have been granted access rights in
19 violation of 45 C.F.R. § 164.312(a)(1);
- 20 f. Failing to implement policies and procedures to prevent, detect, contain and
21 correct security violations in violation of 45 C.F.R. § 164.308(a)(1);
- 22 g. Failing to identify and respond to suspected or known security incidents and
23 failing to mitigate, to the extent practicable, harmful effects of security
24 incidents that are known to the covered entity in violation of 45 C.F.R. §
25 164.308(a)(6)(ii);
- 26 h. Failing to effectively train all staff members on the policies and procedures
27 with respect to PHI as necessary and appropriate for staff members to carry
28 out their functions and to maintain security of PHI in violation of 45 C.F.R.
§ 164.530(b) and 45 C.F.R. § 164.308(a)(5); and
- i. Failing to design, implement, and enforce policies and procedures
establishing physical and administrative safeguards to reasonably safeguard
PHI, in compliance with 45 C.F.R. § 164.530(c).

F. PracticeMax Failed to Adhere to FTC Guidelines

78. According to the Federal Trade Commission (“FTC”), the need for data security should be factored into all business decision-making.²⁰ To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as PracticeMax, should employ to protect against the unlawful exposure of Personal Information.

79. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business.²¹ The guidelines explain that businesses should:

- a. protect the personal customer information that they keep;
- b. properly dispose of personal information that is no longer needed;
- c. encrypt information stored on computer networks;
- d. understand their network’s vulnerabilities; and
- e. implement policies to correct security problems.

80. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

81. The FTC recommends that companies not maintain PHI longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for

²⁰ *Start with Security: A Guide for Business*, FED. TRADE COMM’N (June 2015), <https://bit.ly/3uSoYWF> (last accessed July 25, 2022).

²¹ *Protecting Personal Information: A Guide for Business*, FED. TRADE COMM’N (Oct. 2016), <https://bit.ly/3u9mzre> (last accessed July 25, 2022).

1 suspicious activity on the network; and verify that third-party service providers have
2 implemented reasonable security measures.²²

3 82. The FTC has brought enforcement actions against businesses for failing to
4 adequately and reasonably protect customer data, treating the failure to employ reasonable
5 and appropriate measures to protect against unauthorized access to confidential consumer
6 data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission
7 Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the
8 measures businesses must take to meet their data security obligations.

9 83. PracticeMax’s failure to employ reasonable and appropriate measures to
10 protect against unauthorized access to patient PHI constitutes an unfair act or practice
11 prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

12 **CLASS ACTION ALLEGATIONS**

13 84. Plaintiffs bring this action pursuant to Federal Rule of Civil Procedure
14 23(b)(2) and (b)(3) on behalf of themselves and all members of the proposed class
15 (“Class”), defined as follows:

16 All individuals residing in the United States whose PHI was
17 compromised in the Data Breach disclosed by PracticeMax.

18 85. The following people are excluded from the Class: (1) any judge or
19 magistrate presiding over this action and members of their families; (2) Defendant,
20 Defendant’s subsidiaries, parents, successors, predecessors, affiliated entities, and any
21 entity in which Defendant or its parent has a controlling interest, and their current or former
22 officers and directors; (3) persons who properly execute and file a timely request for
23 exclusion from the Class; (4) persons whose claims in this matter have been finally
24 adjudicated on the merits or otherwise released; (5) Plaintiff’s counsel and Defendant’s
25

26
27 ²² See *Start with Security*.

1 counsel; and (6) the legal representatives, successors, and assigns of any such excluded
2 persons.

3 86. The Class defined above is identifiable through Defendant's business
4 records.

5 87. Plaintiffs reserve the right to amend the Class definition or add a Class if
6 further information and discovery indicate that other classes should be added and if the
7 definition of the Class should be narrowed, expanded, or otherwise modified.

8 88. Plaintiffs and members of the Class satisfy the numerosity, commonality,
9 typicality, and adequacy requirements under Fed. R. Civ. P. 23.

10 89. **Numerosity.** The exact number of the members of the Class is unknown but,
11 upon information and belief, the number exceeds 150,000, and individual joinder in this
12 case is impracticable. Members of the Class can be easily identified through Defendant's
13 records and objective criteria permitting self-identification in response to notice, and notice
14 can be provided through techniques similar to those customarily used in other data breach,
15 consumer breach of contract, unlawful trade practices, and class action controversies

16 90. **Commonality and Predominance.** There are many questions of law and
17 fact common to the claims of Plaintiffs and the Class, and those questions predominate
18 over any questions that may affect individual members of the Class. Common questions
19 for the Class include, but are not necessarily limited to the following:

- 20 a. Whether Defendant had a duty to use reasonable care to safeguard Plaintiffs'
21 and members of the Class's PHI;
- 22 b. Whether Defendant breached the duty to use reasonable care to safeguard
23 members of the Class's PHI;
- 24 c. Whether Defendant knew or should have known about the inadequacies of
25 its data security policies and system and the dangers associated with storing
26 sensitive PHI;
- 27 d. Whether Defendant failed to use reasonable care and commercially
28 reasonable methods to safeguard and protect Plaintiffs' and members of the
Class's PHI from unauthorized release and disclosure;

- e. Whether the proper data security measures, policies, procedures, and protocols were in place and operational within Defendant's computer systems to safeguard and protect Plaintiffs' and members of the Class's PHI from unauthorized release and disclosure;
- f. Whether Defendant took reasonable measures to determine the extent of the Data Breach after it was discovered;
- g. Whether Defendant's delay in informing Plaintiffs and members of the Class of the Data Breach was unreasonable;
- h. Whether Defendant's method of informing Plaintiffs and other members of the Class of the Data Breach was unreasonable;
- i. Whether Defendant's conduct was likely to deceive the public;
- j. Whether Defendant is liable for negligence or gross negligence;
- k. Whether Defendant's conduct, practices, statements, and representations about the Data Breach of the PHI violated applicable state laws;
- l. Whether Plaintiffs and members of the Class were injured as a proximate cause or result of the Data Breach;
- m. Whether Plaintiffs and members of the Class were damaged as a proximate cause or result of Defendant's breach of its contract with Plaintiffs and members of the Class;
- n. What the proper measure of damages is; and,
- o. Whether Plaintiffs and members of the Class are entitled to restitutionary, injunctive, declaratory, or other relief.

91. **Typicality.** Plaintiffs' claims are typical of the claims of other members of the Class in that Plaintiffs, and the members of the Class sustained damages arising out of Defendant's Data Breach, wrongful conduct, concealment, and unlawful practices, and Plaintiffs and members of the Class sustained similar injuries and damages, as a result of Defendant's uniform illegal conduct.

92. **Adequacy of Representation.** Plaintiffs will fairly and adequately represent and protect the interests of the Class and have retained counsel competent and experienced in complex class actions to vigorously prosecute this action on behalf of the Class.

1 Plaintiffs have no interests that conflict with, or are antagonistic to those of, the Class, and
 2 Defendant has no defenses unique to Plaintiffs.

3 93. **Superiority of Class Action.** A class action is also a fair and efficient
 4 method of adjudicating the controversy because class proceedings are superior to all other
 5 available methods for the fair and efficient adjudication of this controversy as joinder of
 6 all parties is impracticable. The damages suffered by the individual members of the Class
 7 will likely be relatively small, especially given the burden and expense of individual
 8 prosecution of the complex litigation necessitated by Defendant's actions. Thus, it would
 9 be virtually impossible for the individual members of the Class to obtain effective relief
 10 from Defendant's misconduct. Even if members of the Class could sustain such individual
 11 litigation, it would still not be preferable to a class action, because individual litigation
 12 would increase the delay and expense to all parties due to the complex legal and factual
 13 controversies presented in this Complaint. By contrast, a class action presents far fewer
 14 management difficulties and provides the benefits of single adjudication, economy of scale,
 15 and comprehensive supervision by a single court. Economies of time, effort, and expense
 16 will be fostered, and uniformity of decisions ensured.

17 94. A class action is therefore superior to individual litigation because:

- 18 a. The amount of damages available to an individual plaintiff is insufficient to
 19 make litigation addressing Defendant's conduct economically feasible in the
 20 absence of the class action procedural device;
- 21 b. Individualized litigation would present a potential for inconsistent or
 22 contradictory judgments, and increases the delay and expense to all parties
 and the court system; and
- 23 c. The class action device presents far fewer management difficulties and
 24 provides the benefits of a single adjudication, economies of scale, and
 25 comprehensive supervision by a single court.

26 95. The litigation of the claims brought herein is manageable. PracticeMax's
 27 uniform conduct, the consistent provisions of the relevant laws, and the ascertainable
 28

identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

96. Adequate notice can be given to Class members directly using information maintained in PracticeMax's records.

97. This proposed class action does not present any unique management difficulties.

98. Further, because Defendant has acted or refused to act on grounds generally applicable to the Class, final injunctive relief and/or corresponding declaratory relief is appropriate for the Class as a whole.

FIRST CAUSE OF ACTION
Negligence
(On Behalf of Plaintiffs and the Class)

99. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

100. Defendant owed to Plaintiffs and other members of the Class a duty to exercise reasonable care in handling and using the PHI in its care and custody, including implementing industry-standard security procedures sufficient to reasonably protect the information from the Data Breach, theft, and unauthorized use that came to pass, and to promptly detect attempts at unauthorized access.

101. Defendant owed a duty of care to Plaintiffs and members of the Class because it was foreseeable that Defendant's failure to adequately safeguard their PHI in accordance with state-of-the-art industry standards concerning data security would result in the compromise of that PHI—just like the Data Breach that ultimately came to pass. Defendant acted with wanton and reckless disregard for the security and confidentiality of Plaintiffs' and members of the Class's PHI by disclosing and providing access to this information to third parties and by failing to properly supervise both the manner in which the PHI was

1 stored, used, and exchanged, and those in its employ who were responsible for making that
2 happen.

3 102. Defendant owed Plaintiffs and members of the Class a duty to notify them
4 within a reasonable time frame of any breach to the security of their PHI. Defendant also
5 owed a duty to timely and accurately disclose to Plaintiffs and members of the Class the
6 scope, nature, and occurrence of the Data Breach. This duty is required and necessary in
7 order for Plaintiffs and members of the Class to take appropriate measures to protect their
8 PHI, to be vigilant in the face of an increased risk of harm, and to take other necessary
9 steps in an effort to mitigate the harm caused by the Data Breach.

10 103. Defendant owed these duties to Plaintiffs and members of the Class because
11 they are members of a well-defined, foreseeable, and probable class of individuals whom
12 Defendant knew or should have known would suffer injury-in-fact from Defendant's
13 inadequate security protocols. Defendant actively sought and obtained Plaintiffs' and
14 members of the Class's personal information and PHI.

15 104. The risk that unauthorized persons would attempt to gain access to the PHI
16 and misuse it was foreseeable. Given that Defendant holds vast amounts of PHI, it was
17 inevitable that unauthorized individuals would attempt to access Defendant's databases
18 containing the PHI.

19 105. PHI is highly valuable, and Defendant knew, or should have known, the risk
20 in obtaining, using, handling, emailing, and storing the PHI of Plaintiffs and members of
21 the Class and the importance of exercising reasonable care in handling it.

22 106. Defendant breached its duties by failing to exercise reasonable care in
23 supervising its agents, contractors, vendors, and suppliers, and in handling and securing
24 the personal information and PHI of Plaintiffs and members of the Class which actually
25 and proximately caused the Data Breach and Plaintiffs' and members of the Class's injury.
26 Defendant further breached its duties by failing to provide reasonably timely notice of the
27 Data Breach to Plaintiffs and members of the Class, which actually and proximately caused
28

1 and exacerbated the harm from the Data Breach and Plaintiffs' and members of the Class's
2 injuries-in-fact. As a direct and traceable result of Defendant's negligence and/or negligent
3 supervision, Plaintiffs and members of the Class have suffered or will suffer damages,
4 including monetary damages, increased risk of future harm, embarrassment, humiliation,
5 frustration, and emotional distress.

6 107. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendant had a duty to provide
7 fair and adequate computer systems and data security practices to safeguard Plaintiffs' and
8 members of the Class's PHI.

9 108. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting
10 commerce," including, as interpreted and enforced by the FTC, the unfair act or practice
11 by businesses, such as Defendant, of failing to use reasonable measures to protect
12 customers or, in this case, patients' PHI. The FTC publications and orders promulgated
13 pursuant to the FTC Act also form part of the basis of Defendant's duty to protect Plaintiffs
14 and the members of the Class's sensitive PII.

15 109. Defendant violated its duty under Section 5 of the FTC Act by failing to use
16 reasonable measures to protect Plaintiffs' and the Class's PHI and not complying with
17 applicable industry standards as described in detail herein. Defendant's conduct was
18 particularly unreasonable given the nature and amount of PHI Defendant had collected and
19 stored and the foreseeable consequences of a data breach, including, specifically, the
20 immense damages that would result to patients in the event of a breach, which ultimately
21 came to pass.

22 110. The harm that has occurred is the type of harm the FTC Act is intended to
23 guard against. Indeed, the FTC has pursued numerous enforcement actions against
24 businesses that, because of their failure to employ reasonable data security measures and
25 avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs
26 and members of the Class.

1 111. Defendant had a duty to Plaintiffs and the members of the Class to implement
2 and maintain reasonable security procedures and practices to safeguard Plaintiffs' and the
3 Class's PII.

4 112. Defendant breached its respective duties to Plaintiffs and members of the
5 Class under the FTC Act by failing to provide fair, reasonable, or adequate computer
6 systems and data security practices to safeguard Plaintiffs' and members of the Class's PII.

7 113. Defendant's violation of Section 5 of the FTC Act and its failure to comply
8 with applicable laws and regulations constitutes negligence *per se*.

9 114. Pursuant to HIPAA (42 U.S.C. § 1302d, *et seq.*), Defendant had a duty to
10 implement reasonable safeguards to protect Plaintiffs' and Class members' PHI.

11 115. Pursuant to HIPAA, Defendant had a duty to render the electronic PHI it
12 maintained unusable, unreadable, or indecipherable to unauthorized individuals, as
13 specified in the HIPAA Security Rule by "the use of an algorithmic process to transform
14 data into a form in which there is a low probability of assigning meaning without use of a
15 confidential process or key" (45 C.F.R. § 164.304 definition of encryption).

16 116. Plaintiffs and Class members are within the class of persons that the HIPAA
17 was intended to protect.

18 117. The harm that occurred as a result of the Data Breach is the type of harm that
19 HIPAA was intended to guard against. The Federal Health and Human Services' Office for
20 Civil Rights ("OCR") has pursued enforcement actions against businesses, which, as a
21 result of their failure to employ reasonable data security measures relating to protected
22 health information, caused the same harm as that suffered by Plaintiffs and the Class
23 members.

24 118. Defendant breached its duties to Plaintiffs and the Class under HIPAA, by
25 failing to provide fair, reasonable, or adequate computer systems and data security
26 practices to safeguard Plaintiffs' and Class members' PHI.

119. Defendant's failure to comply with applicable laws and regulations constitutes negligence *per se*.

120. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

121. Defendant's breach of its common-law duties to exercise reasonable care and its duties under Section 5 of the FTC Act and HIPAA actually and proximately caused Plaintiff's and members of the Class's actual, tangible, injury-in-fact and damages, including, without limitation, the theft of their PHI by criminals, improper disclosure of their PHI, lost benefit of their bargain, lost value of their PHI, and lost time and money incurred to mitigate and remediate the effects of the Data Breach that resulted from and were caused by Defendant's negligence, which injury-in-fact and damages are ongoing, imminent, immediate, and which they continue to face.

SECOND CAUSE OF ACTION
Arizona Consumer Fraud Act,
A.R.S. §§ 44-1521, *et seq.*
(On Behalf of Plaintiffs and the Class)

122. Plaintiffs and members of the Class incorporate the above allegations as if fully set forth herein.

123. Defendant is a "person" as defined by A.R.S. §44-1521(6).

124. Defendant sold Plaintiffs and Class members "merchandise" as that term is defined by A.R.S. § 44-1521, in the form of services, including medical billing and records services.

125. Section 44-1522 of the Arizona Consumer Fraud Act provides:

The act, use or employment by any person of any deception, deceptive or unfair act or practice, fraud, false pretense, false promise, misrepresentation, or concealment, suppression or omission of any material fact with intent that others rely on such concealment, suppression or omission, in connection with the sale or advertisement of any merchandise whether or not any person has in fact been misled, deceived or damaged thereby.

See A.R.S. § 44-1522(A).

1 126. Defendant used deception, used a deceptive act or practice, and fraudulently
2 omitted and concealed material facts in connection with the sale or advertisement of that
3 merchandise in violation of A.R.S. § 44-1522(A).

4 127. Defendant omitted and concealed material facts, which it knew about and
5 had the duty to disclose—namely, Defendant’s inadequate privacy and security protections
6 for Plaintiffs’ and Class members’ PHI. This omission was designed to mislead consumers.

7 128. Defendant omitted and concealed those material facts even though in equity
8 and good conscience those facts should have been disclosed and did so with the intent that
9 others would rely on the omission, suppression, and concealment.

10 129. The concealed facts are material in that they are logically related to the
11 transactions at issue and rationally significant to the parties in view of the nature and
12 circumstances of those transactions.

13 130. Plaintiffs do not allege any claims based on any affirmative
14 misrepresentations by Defendant; rather, Plaintiffs allege that Defendant omitted, failed to
15 disclose, and concealed material facts and information as alleged herein, despite its duty to
16 disclose such facts and information.

17 131. Defendant knew or should have known that its computer system and data
18 security practices were inadequate to safeguard Plaintiffs’ and Class members’ PHI, and
19 that the risk of a data breach or theft was highly likely. Defendant’s actions in engaging in
20 these deceptive acts and practices were intentional, knowing and willful, and wanton and
21 reckless with respect to the rights of Plaintiffs and Class members.

22 132. Specifically, Defendant failed to comply with the standards outlined by the
23 FTC and HIPAA regarding protecting PHI. Defendant was or should have been aware of
24 these standards. Defendant’s data security systems did not follow the FTC’s guidelines and
25 HIPAA’s Administrative Simplification Rules and, as a result, were operating below the
26 minimum standards set forth.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: July 27, 2022

Respectfully submitted,

/s/Elaine A. Ryan

Elaine A. Ryan (AZ Bar #012870)

Colleen M. Auer (AZ Bar#014637)

AUER RYAN, P.C.

20987 N. John Wayne Parkway, #B104-374

Maricopa, AZ 85139

520-705-7332

eryan@auer-ryan.com

cauer@auer-ryan.com

TURKE & STRAUSS LLP

Samuel J. Strauss*

Raina C. Borrelli*

613 Williamson St., Suite 201

Madison, WI 53703

T: (608) 237-1775

F: (608) 509-4423

sam@turkestrauss.com

raina@turkestrauss.com

* to seek admission *pro hac vice*

Counsel for Plaintiffs and the Proposed Class

EXHIBIT A



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
 <<address_1>>
 <<address_2>>
 <<city>>, <<state_province>> <<postal_code>>
 <<country>>

<<b2b_text_1(NOTICE OF DATA INCIDENT / NOTICE OF DATA BREACH)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

PracticeMax is a business management and information technology solutions company. We provide services including billing, consulting, registration, and other solutions to companies, including hospitals, insurance companies, employers, and physician offices, and as a result we are in possession of some information related to you. This letter contains information about a data incident at PracticeMax. The letter also provides information about our response and resources available to help protect information, should you feel it is appropriate to do so.

What Happened? On May 1, 2021, PracticeMax became aware of technical issues relating to systems in the PracticeMax network. We promptly commenced an investigation and identified ransomware on certain systems. We disconnected our systems and partnered with subject matter specialists to assist with our investigation and to confirm the security of our network. We began restoring the network and business operations, and we implemented additional security policies and controls. We also communicated the incident to our customers.

The investigation determined the PracticeMax network was subject to unauthorized access beginning on April 17, 2021 until May 5, 2021 and during that time one server was accessed and certain files may have been removed. The investigation also identified unauthorized access to a limited number of company email accounts. We reviewed the server and email accounts for sensitive information and determined these systems may have contained sensitive information at the time of the incident. Although the investigation did not identify evidence confirming any unauthorized access, acquisition, or disclosure of sensitive information, we cannot rule out the possibility of such activity. Additionally, some of the data stored in our network was encrypted as a result of the ransomware.

What Information Was Involved? In general, we collect demographic and health information, including but not limited to name, address, Social Security number, date of birth, treatment and/or diagnosis information, health insurance information and, in some cases, financial information for individuals associated with our customers. The information varies depending on what was provided to PracticeMax, however, it is possible these types of information may have been present on the involved systems at the time of the incident. Importantly, our investigation did not identify evidence of unauthorized access, acquisition, or disclosure of your information, however, the review of the involved systems identified information including your <<b2b_text_2(name, data elements)>><<b2b_text_3(data elements cont.)>>.

What We Are Doing. PracticeMax is committed to safeguarding information and has strict security measures in place to protect information in our care. Upon learning of this incident, we moved quickly to investigate and respond and to confirm the security of our systems. As part of PracticeMax's ongoing commitment to the privacy of information in our care, we reviewed our existing policies and procedures and implemented additional safeguards to further our already stringent security policies and procedures and to secure the information in our systems. We also notified law enforcement, our customers, and relevant regulators of this incident.

What You Can Do. We encourage you to remain vigilant by reviewing documents for suspicious activity, including health insurance statements, explanation of benefits of letters, medical records, account statements and credit reports. If you find unfamiliar activity on statements you receive from your health insurance company, you should immediately notify your health insurance company. Additionally, any suspicious activity on your credit report should be reported immediately to law enforcement. You can also review the enclosed *Steps You Can Take To Help Protect Personal Information* for more information.

If you have additional questions, please call our dedicated assistance line at (855) 568-2073 (toll free), Monday through Friday, 9:00 a.m. to 6:30 p.m. Eastern Time (excluding some U.S. holidays).

Sincerely,

Michael Johnson

CEO

PracticeMax

STEPS YOU CAN TAKE TO HELP PROTECT PERSONAL INFORMATION

Monitor Your Accounts

Under U.S. law, a consumer is entitled to one free credit report annually from each of the three major credit reporting bureaus, Equifax, Experian, and TransUnion. To order your free credit report, visit www.annualcreditreport.com or call, toll-free, 1-877-322-8228. You may also directly contact the three major credit reporting bureaus listed below to request a free copy of your credit report.

Consumers have the right to place an initial or extended “fraud alert” on a credit file at no cost. An initial fraud alert is a 1-year alert that is placed on a consumer’s credit file. Upon seeing a fraud alert display on a consumer’s credit file, a business is required to take steps to verify the consumer’s identity before extending new credit. If you are a victim of identity theft, you are entitled to an extended fraud alert, which is a fraud alert lasting seven years. Should you wish to place a fraud alert, please contact any one of the three major credit reporting bureaus listed below.

As an alternative to a fraud alert, consumers have the right to place a “credit freeze” on a credit report, which will prohibit a credit bureau from releasing information in the credit report without the consumer’s express authorization. The credit freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. However, you should be aware that using a credit freeze to take control over who gets access to the personal and financial information in your credit report may delay, interfere with, or prohibit the timely approval of any subsequent request or application you make regarding a new loan, credit, mortgage, or any other account involving the extension of credit. Pursuant to federal law, you cannot be charged to place or lift a credit freeze on your credit report. To request a credit freeze, you will need to provide the following information:

1. Full name (including middle initial as well as Jr., Sr., II, III, etc.);
2. Social Security number;
3. Date of birth;
4. Addresses for the prior two to five years;
5. Proof of current address, such as a current utility bill or telephone bill;
6. A legible photocopy of a government-issued identification card (state driver’s license or ID card, etc.); and
7. A copy of either the police report, investigative report, or complaint to a law enforcement agency concerning identity theft if you are a victim of identity theft.

Should you wish to place a credit freeze, please contact the three major credit reporting bureaus listed below:

Equifax	Experian	TransUnion
https://www.equifax.com/personal/credit-report-services/	https://www.experian.com/help/	https://www.transunion.com/credit-help
888-298-0045	1-888-397-3742	833-395-6938
Equifax Fraud Alert, P.O. Box 105069 Atlanta, GA 30348-5069	Experian Fraud Alert, P.O. Box 9554, Allen, TX 75013	TransUnion Fraud Alert, P.O. Box 2000, Chester, PA 19016
Equifax Credit Freeze, P.O. Box 105788 Atlanta, GA 30348-5788	Experian Credit Freeze, P.O. Box 9554, Allen, TX 75013	TransUnion Credit Freeze, P.O. Box 160, Woodlyn, PA 19094

Additional Information

As a general practice, we encourage individuals to frequently reset online account passwords, to use complex password combinations, and to not share passwords or use identical passwords for multiple online accounts. You may further educate yourself regarding identity theft, fraud alerts, credit freezes, and the steps you can take to protect your personal information by contacting the consumer reporting bureaus, the Federal Trade Commission, or your state Attorney General. The Federal Trade Commission may be reached at: 600 Pennsylvania Avenue NW, Washington, DC 20580; www.identitytheft.gov; 1-877-ID-THEFT (1-877-438-4338); and TTY: 1-866-653-4261. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them. You can obtain further information on how to file such a complaint by way of the contact information listed above. You have the right to file a police report if you ever experience identity theft or fraud. Please note that in order to file a report with law enforcement for identity theft, you will likely need to provide some proof that you have been a victim. Instances of known or suspected identity theft should also be reported to law enforcement and your state Attorney General. This notice has not been delayed by law enforcement.

For District of Columbia residents, the District of Columbia Attorney General may be contacted at: 400 6th Street, NW, Washington, DC 20001; 202-727-3400; and oag@dc.gov.

For Maryland residents, the Maryland Attorney General may be contacted at: 200 St. Paul Place, 16th Floor, Baltimore, MD 21202; 410-576-6300 or 1-888-743-0023; and www.oag.state.md.us. PracticeMax is located at 1440 East Missouri Avenue, Suite C-200, Phoenix, AZ 85014.

For New Mexico residents, you have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the consumer reporting bureaus must correct or delete inaccurate, incomplete, or unverifiable information; consumer reporting agencies may not report outdated negative information; access to your file is limited; you must give your consent for credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. We encourage you to review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

For New York residents, the New York Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; or <https://ag.ny.gov/>.

For North Carolina residents, the North Carolina Attorney General may be contacted at: 9001 Mail Service Center, Raleigh, NC 27699-9001; 1-877-566-7226 or 1-919-716-6000; and www.ncdoj.gov.

For Rhode Island residents, the Rhode Island Attorney General may be reached at: 150 South Main Street, Providence, RI 02903; www.riag.ri.gov; and 1-401-274-4400. Under Rhode Island law, you have the right to obtain any police report filed in regard to this incident. There are [#] Rhode Island residents impacted by this incident.